Mettre son entreprise en conformité avec la CNIL, secrets et mode d’emploi

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations ici : https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés.- Que se cache derrière cette loi ?

– Quels sont les étapes indispensables et les pièges à éviter pour que cette mise en conformité ne se transforme pas en fausse déclaration ?

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84

Datadock Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.
« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

Quelques articles sélectionnés par nos Experts :
Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : Denis JACOPINI

Lutte contre le blanchiment d’argent : quelles formalités à la CNIL ? | Denis JACOPINI

Lutte contre le blanchiment d’argent : quelles formalités à la CNIL ?

Les fichiers relatifs à la lutte contre le blanchiment d'argent et le financement du terrorisme mis en oeuvre par les organismes financiers doivent être déclarés à la CNIL :

• Par une déclaration simplifiée de conformité à l'autorisation unique 003 si le fichier correspond aux caractéristiques énoncées dans ce texte ;
• Par une demande d'autorisation si le fichier sort du cadre de cette norme.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.aide.cnil.fr/selfcnil/site/template.do?id=537&back=true

Vidéosurveillance en entreprise : règles et limites | Denis JACOPINI

#Vidéosurveillance en entreprise : règles et limites

Un système de vidéosurveillance en entreprise se doit d'observer certaines limites pour rester dans un cadre de protection des biens et personnes.

Le cadre législatif de la vidéosurveillance
C'est la loi dite « informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004, qui fixe le cadre de mise en place d'une vidéosurveillance sur un lieu à usage professionnel.
Ainsi dans des lieux non accessibles au public (bureaux, entrepôts, réserves, locaux d'administration) l'installation d'une vidéosurveillance doit faire l'objet d'une déclaration à la CNIL (Commission Nationale Informatique et Libertés).
C'est également une obligation pour les guichets de réception de clients et les commerces, lorsque le système enregistre les images dans un fichier et permettant de conserver d'identité des personnes filmées.
Si toutefois les fichiers ne sont pas conservés à des fins d'identification, un assouplissement de la loi permet de solliciter une simple autorisation préfectorale (pour les lieux accueillant du public).

Information des salariés et du public
Une information préalable est requise auprès des représentants des salariés avant tout installation d'un dispositif de vidéosurveillance, en mettant l'accent sur les objectifs de sécurité et en spécifiant que les enregistrements ne sont pas conservés plus d'un mois.
De la même manière, l'entreprise doit mettre en place une signalisation informant les visiteurs de la présence d'un système de vidéosurveillance.
Cet affichage doit se faire dès l'entrée dans l'établissement, en précisant les raisons ainsi que les coordonnées de l'autorité ou de la personne chargée de l'exploitation du système et en rappelant les modalités d'exercice du droit d'accès des personnes filmées aux enregistrements qui les concernent (loi du 6 août 2004).

Le principe de proportionnalité
On pourrait dire aussi principe de bon sens. L'employeur doit en premier lieu démontrer l'intérêt légitime à la mise en place d'un système de surveillance. Il peut s'agir de la nécessité de protéger des personnes ou des biens, ou de se prémunir contre des risques tels que le vol.
Partant de là, le dispositif installé doit être proportionnel au regard des intérêts à protéger.
Il y a une différence notoire entre installer une caméra dans un entrepôt à des fins de sécurité et le fait d'en installer une permettant d'observer en permanence des postes de travail.
Bien évidemment des caméras installées dans des lieux de repos des salariés ou dans des toilettes constituent une surveillance excessive. La CNIL a récemment mis à l'amende des entreprises pour des situations de surveillance jugées excessives et non proportionnées par rapport aux risques à prévenir.
La CNIL a fait valoir que des caméras peuvent être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation, ou encore filmer les zones où de la marchandise ou des biens de valeur sont entreposés. Pas question en revanche de filmer en permanence un employé sur son poste de travail, sauf si celui-ci manipule par exemple de l'argent, en vertu du principe de proportionnalité.
En synthèse, bien que frappée du sceau du bon sens, la mise en place d'un système de vidéosurveillance doit s'accompagner de certaines précautions. Eventuellement prenez avis auprès de votre conseiller en assurances, qui saura vous orienter vers un prestataire de vidéosurveillance homologué et bien au fait des contraintes législatives.

Source :
http://www.comptanoo.com/assurance-prevention/actualite-tpe-pme/23794/videosurveillance-entreprise-regles-et-limites

Règlement européen sur la protection des données : Transparence et responsabilisation

	Règlement européen sur la protection des données : Transparence et responsabilisation

Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

Une clé de lecture : la protection des données dès la conception et par défaut (*privacy by design*)

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (*accountability*).

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les études d'impact sur la vie privée (EIVP)

Les « études d'impact sur la vie privée » (EIVP ou PIA)

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

Si l'organisme ne parvient pas à réduire ce risque élevé par des mesures appropriées, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures.

L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

Le Délégué à la Protection des données (*Data Protection Officer*)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

source : CNIL

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger**pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Règlement européen sur la protection des données : Renforcement des droits des personnes

	Règlement européen sur la protection des données : Renforcement des droits des personnes

Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.

Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

source : CNIL

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger**pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Règlement européen sur la

protection des données : Evolution du cadre juridique

	Règlement européen sur la protection des données : Evolution du cadre juridique

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne le 4 mai 2016 et entré en application le 25 mai 2018. L'adoption de ce texte permet à l'Europe de s'adapter aux nouvelles réalités du numérique.

Un cadre juridique unifié pour l'ensemble de l'UE

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu

• Le critère du ciblage

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

• La responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le projet de règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational – donc qu'il concernera les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernées seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

• **Par exemple**, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État. Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

source : CNIL

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Géolocalisation des véhicules de l’entreprise : la CNIL modifie la donne ! | Denis JACOPINI

Géolocalisation des véhicules de l’entreprise : la CNIL modifie la donne !

La CNIL avait adopté en 2006 une norme simplifiée permettant à tout employeur de recourir à un dispositif de géolocalisation tout en respectant les libertés individuelles des salariés. La CNIL vient à présent d'apporter des modifications significatives à cette norme, notamment en matière de contrôle du temps de travail.

Géolocalisation d'un salarié : les règles à suivre

La géolocalisation est un procédé qui équipe les véhicules d'entreprise d'un dispositif GPS permettant leur localisation géographique immédiate. Dans le BTP, il peut être utilisé, par exemple, pour contrôler et vérifier les déplacements du personnel de chantier.

Il est possible d'y recourir à condition de ne pas aboutir à un contrôle permanent du salarié.

La mise en œuvre du dispositif de géolocalisation doit être proportionnelle au but recherché et justifiée par l'activité de l'entreprise. Le CE doit être informé et consulté (ou à défaut les DP), préalablement à tout projet de mise en place d'un dispositif de géolocalisation au sein des véhicules de l'entreprise. Ensuite, vous devrez en informer l'ensemble du personnel (lettre remise en mains propres, note de service, etc.).

Pour cela, les Editions Tissot mettent à votre disposition un modèle d'attestation d'information de mise en place d'un système de géolocalisation extrait de la documentation « Formulaire Social BTP commenté ».

Il faut également déclarer le dispositif à la CNIL.

La CNIL a en effet adopté en 2006, une recommandation portant sur la géolocalisation des véhicules utilisés par les salariés. L'objectif étant d'encadrer la mise en œuvre d'un tel dispositif tout en respectant la loi relative à l'informatique et aux libertés mais également au Code du travail. De cette recommandation est née une norme simplifiée dite « Norme 51 ».

Ainsi, dès lors que vous souhaitez équiper vos véhicules d'un système de géolocalisation, vous devez au préalable effectuer une déclaration de conformité à la norme 51 auprès de la CNIL afin d'attester que vous respectez scrupuleusement ce que prescrit la CNIL.

Or cette norme 51 vient d'être modifiée par la CNIL.

Géolocalisation : les principales modifications apportées par la CNIL

La nouvelle norme du 4 juin 2015, consolidée le 29 juin 2015, vous défend de collecter des données de géolocalisation durant le trajet domicile/travail mais également pendant le temps de pause de vos salariés. En effet, la précédente norme précisait seulement que le salarié avait la possibilité de désactiver le dispositif en dehors de son temps de travail ou bien durant son temps de pause.

En revanche, cette nouvelle norme rend possible la désactivation par le salarié du dispositif et ce à tout moment de la journée. En effet, l'article 6 de ladite norme précise que : « les employés doivent avoir la possibilité de désactiver la fonction de géolocalisation des véhicules, en particulier à l'issue de leur temps de travail ou pendant leur temps de pause ».

Toutefois, ce droit dont bénéficie le salarié s'accompagne d'une contrepartie vous permettant de recueillir toutes explications de sa part en cas de désactivations trop fréquentes.

Par ailleurs, s'agissant du recueil des données traitées, il est possible de collecter la date ainsi que l'heure d'une activation ou d'une désactivation du dispositif par le salarié et ce durant le temps de travail. En conséquence, une procédure disciplinaire pourrait être engagée à l'encontre d'un salarié qui désactive fréquemment le dispositif de géolocalisation sans raison valable.

Enfin, la norme vous rappelle que le dispositif de géolocalisation n'a pas pour objectif de contrôler la vitesse de vos salariés. En effet, vous ne pourrez relever des infractions aux dispositions relatives au Code de la route puisque celles-ci ont trait à des données à caractère personnel que seuls les agents de services compétents peuvent sanctionner.

Source : http://www.batiactu.com/edito/geolocalisation-vehicules-entreprise-cnil-modifie-donne-42230.php

Dispositif biométrique d’accès à la cantine : quelles formalités à la CNIL ? | Denis JACOPINI

Dispositif biométrique d’accès à la cantine : quelles formalités à la CNIL ?

Les dispositifs biométriques utilisant le contour de la main des élèves pour gérer l’accès à la cantine scolaire sont couverts par une autorisation unique adoptée par la CNIL.

Les établissements qui souhaitent installer ce type de dispositifs doivent faire une déclaration simplifiée, en sélectionnant dans l’onglet « Finalité » l’autorisation unique AU-009.
Le responsable du dispositif s’engage ainsi à se conformer aux caractéristiques décrites dans ce texte.
Les autres dispositifs biométriques (réseaux veineux, empreintes digitales, reconnaissance faciale, etc.) doivent faire l’objet d’une demande d’autorisation préalable auprès de la CNIL.
Lire la suite….

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d’abord commencer par un Audit de l’ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do?name=Dispositif+biom%C3%A9trique+d%27acc%C3%A8s+%C3%A0+la+cantine+%3A+quelles+formalit%C3%A9s+%C3%A0+la+CNIL+%3F&id=281

Coronavirus (Covid-19) : Ce que les employeurs doivent faire (ou pas) vis à vis de la CNIL

Dans le contexte de crise sanitaire liée au coronavirus, particuliers et professionnels s'interrogent sur les mesures à mettre en œuvre aux fins de limiter la propagation du virus, et sur les conditions dans lesquelles les données personnelles, notamment de santé, peuvent être utilisées. La CNIL rappelle quelques principes.

Ce qu'il ne faut pas faire

Si chacun doit mettre en œuvre des mesures adaptées à la situation telles que la limitation des déplacements et réunions ou encore le respect de mesures d'hygiène, les employeurs ne peuvent pas prendre des mesures susceptibles de porter atteinte au respect de la vie privée des personnes concernées, notamment par la collecte de données de santé qui iraient au-delà de la gestion des suspicions d'exposition au virus. Ces données font en effet l'objet d'une protection toute particulière, tant par le RGPD que par les dispositions du Code de la santé publique.

Par exemple, **les employeurs doivent s'abstenir de collecter de manière systématique et généralisée, ou au travers d'enquêtes et demandes individuelles, des informations relatives à la recherche d'éventuels symptômes présentés par un employé/agent et ses proches.**

Il n'est donc pas possible de mettre en œuvre, par exemple :

• **des relevés obligatoires des températures corporelles de chaque employé/agent/visiteur à adresser quotidiennement à sa hiérarchie ;**

• **ou encore, la collecte de fiches ou questionnaires médicaux auprès de l'ensemble des employés/agents.**

Ce qu'il est possible de faire

L'employeur est responsable de la santé et de la sécurité des salariés/agents conformément au Code du travail et des textes régissant la fonction publique (particulièrement l'article L. 4121-1 du Code du travail). Il doit, à ce titre, mettre en œuvre des actions de prévention des risques professionnels, des actions d'information et de formation, et enfin mettre en place une organisation et des moyens adaptés.

Dans ce contexte, l'employeur peut :

• **sensibiliser et inviter ses employés à effectuer des remontées individuelles d'information les concernant en lien avec une éventuelle exposition, auprès de lui ou des autorités sanitaires compétentes ;**

• **faciliter leur transmission par la mise en place, au besoin, de canaux dédiés ;**

• **favoriser les modes de travail à distance et encourager le recours à la médecine du travail.**

En cas de signalement, un employeur peut consigner :

• la date et l'identité de la personne suspectée d'avoir été exposée ;

• les mesures organisationnelles prises (confinement, télétravail, orientation et prise de contact avec le médecin du travail, etc.).

Il pourra ainsi communiquer aux autorités sanitaires qui le demanderaient les éléments liés à la nature de l'exposition, nécessaires à une éventuelle prise en charge sanitaire ou médicale de la personne exposée.

Les entreprises et administrations peuvent également être amenées à établir un « plan de continuité de l'activité » (PCA), qui a pour objectif de maintenir l'activité essentielle de l'organisation. Ce plan doit notamment prévoir toutes les mesures pour protéger la sécurité des employés, identifier les activités essentielles devant être maintenues et également les personnes nécessaires à la continuité du service.

Chaque employé/agent doit pour sa part mettre en œuvre tous les moyens afin de préserver la santé et la sécurité d'autrui et de lui-même (article L.4122-1 du Code du travail) : **il doit informer son employeur en cas de suspicion de contact avec le virus**.

Enfin, **des données de santé peuvent être collectées par les autorités sanitaires**, qualifiées pour prendre les mesures adaptées à la situation. L'évaluation et la collecte des informations relatives aux symptômes du coronavirus et des informations sur les mouvements récents de certaines personnes relèvent de la responsabilité de ces autorités publiques.

Si la situation sanitaire exige de l'ensemble des acteurs qu'ils fassent preuve d'une vigilance particulière, la CNIL invite particuliers et professionnels à suivre les recommandations des autorités sanitaires et à effectuer uniquement les collectes de données sur la santé des individus qui auraient été sollicitées par les autorités compétentes.

Suivez et relayez les recommandations sanitaires sur le site du Gouvernement

Questions/réponses pour les entreprises et les salariés sur travail-emploi.gouv.fr

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

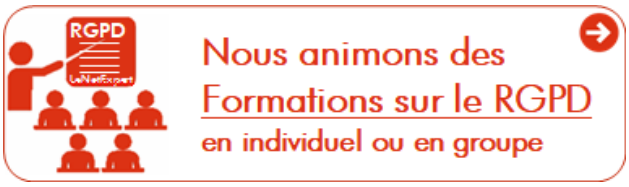
Contactez-nous

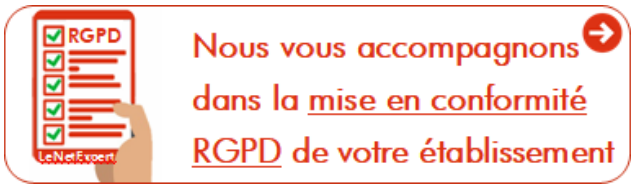
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : *Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles | CNIL*

Ce document à pour objectif de relayer la recommandation de la CNIL.

Comment démarrer une mise en conformité avec le RGPD ? Les conseils de notre Expert

Comment démarrer une mise en conformité avec le RGPD ? Les conseils de notre Expert

Une démarche de mise en conformité avec le RGPD peut à la fois être simple et compliquée.
Une démarche de mise en conformité avec le RGPD peut à la fois être simple (pour de petites structures manipulant un simple carnet d'adresse) et compliquée (pour des structures manipulant des données bancaires, médicales, sociales, juridiques, fiscales)….

PETIT RAPPEL

Le RGPD (règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE), signifie **R**ègleme**n**t **G**énéral sur la **P**rotection des **D**onnées.
Ce règlement qui doit être respecté depuis le 26 avril 2016 avec des sanctions possible depuis le 25 mai 2018 est basé à 90% sur des règles datant de 1978 (c.f. Loi Informatique et Libertés du 6 janvier 1978 qui contient quasiment tout le contenu du RGPD).
Sont concernées toutes les entreprises, toutes les administrations et toutes les associations situées dans l'UE ou manipulant des données à caractère personnel de personnes situées dans l'UE.
Autant dire que tout le monde est concerné (de la grande à la micro structure) sauf les particuliers manipulant des données à caractères personnel exclusivement pour un usage privé.

EN QUOI CONSISTE UNE DEMARCHE DE MISE EN CONFORMITE AVEC LE RGPD ?

Une mise en conformité en tant que telle et définitive n'existe pas. La mise en conformité RGPD est en fait une démarche d'amélioration régulière en vue de respecter des règles parfois difficilement atteignables
Il s'agit donc d'abord d'une analyse de l'existant (avec un éventuel audit), puis de corrections initiales pour enfin prévoir un suivi régulier à la recherche d'améliorations éventuelles.

QUEL EST SON CHAMP D'APPLICATION ?

Un site Internet n'est qu'un point d'entrée parmi d'autres d'informations à destination des traitements de données à caractère personnel que vous réalisez.
La démarche de mise en conformité RGPD doit couvrir à la fois tous les points d'entrée, tous les lieux de traitement et de stockage des données à caractère personnel ainsi que toutes les actions destinées à communiquer à d'autres tiers de telles informations et ceci d'un point de vue technique et juridique.
La démarche couvrira aussi bien vos locaux, votre système informatique, votre site internet, vos services dans le cloud etc.

QUELLE EST NOTRE METHODE ?

Nous avons une méthode consistant à **nous adapter aux ressources humaines et aux compétences existantes au sein de votre structure**.
En effet, plusieurs situations peuvent donc se présenter à nous face auxquelles **nous nous adapterons** :
1. Si vous avez une ressource interne en mesure d'apprendre et de devenir autonome, nous pouvons former cette ressource.
2. Si vous n'avez aucune ressource interne en mesure d'assurer cette démarche de mise en conformité, nous pourrons nous charger de vous accompagner dans toutes vos démarches de mise en conformité.
3. Si vous avez une ressource interne ou des prestataires en mesure de réaliser une partie du travail de recensement et de suivi, nous accompagnerons et ferons progresser cette personne en l'aidant à réaliser cette démarche de mise en conformité.

NOTRE PRIX

Le prix est le résultat de nombreux paramètres tels que :
– la taille de votre structure,
– le volume d'information traitées,
– le type d'informations traitées,
– le type système de traitement de données à caractère personnel utilisé,
– le niveau de conformité de votre système de traitement de données à caractère personnel utilisé par rapport aux différentes réglementations,
– votre situation géographique si nous devons nous déplacer.

LE PRIX GLOBAL

Le prix global d'une démarche de mise en conformité avec le RGPD dépendra avant tout :
• de l'état de votre structure avant le démarrage de la mise en conformité avec une ou plusieurs réglementations (un audit sera probablement nécessaire),
• du nombre de réglementations à respecter et à auditer,
• des démarches que vous souhaitez mettre en oeuvre avec les différents fournisseurs et prestataires concernés par ces améliorations,
• de la densité du planning que vous avez décidé de suivre.
• et enfin du type d'accompagnement que vous attendez de nous (au plus vous en faîtes, au plus le coût sera réduit).
Denis JACOPINI, Expert informatique diplômé en Cybercriminalité et spécialisé en RGPD est en mesure de vous accompagner dans vos démarches de mise en conformité, que votre structure ait une implantation nationale ou internationale.
En savoir plus sur Denis JACOPINI
Contacter Denis JACOPINI

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

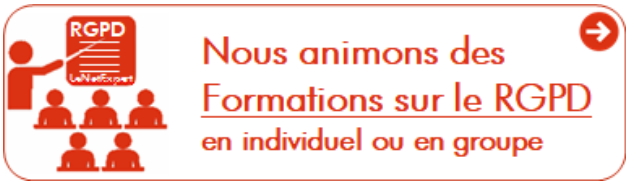
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

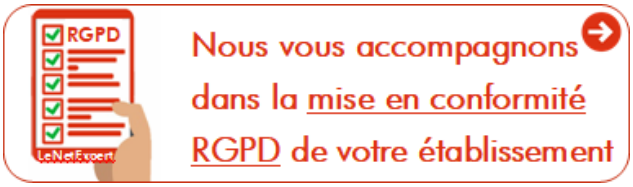
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]